Opinnäytetyö (AMK)

Tietojenkäsittely

Tietojärjestelmät

2010

Antti Laine

TIETOTURVAKARTOITUS JA TIETOTURVATASON NOSTAMINEN

– Hallinnollinen tietoturva pienorganisaatiossa

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietojärjestelmät

Huhtikuu 2011 | 39 sivua

Ohjaaja: Tuomo Helo

Antti Laine

TIETOTURVAKARTOITUS JA TIETOTURVATASON NOSTAMINEN – HALLINNOLLINEN TIETOTURVA PIENORGANISAATIOSSA

Työssä tutkitaan tietoturvakartoituksen tekemistä ja tietoturvatason nostamista pienorganisaatiossa, pääpainona hallinnollinen tietoturva. Tarkoituksena on nostaa Yhdistys X:n tietoturvan tasoa ja antaa sille työkalut sen ylläpitämiseen.

Ensimmäisessä osassa käsitellään yleisesti tietoturvaa ja tarkastellaan hallinnollista tietoturvaa tarkemmin. Tietoturvapolitiikka, toipumissuunnitelmat ja riskien hallinta ovat oleellinen osa hallinnollista tietoturvaa.

Seuraavassa osassa keskitytään organisaation tietoturvan tason tutkimiseen ja hyviin periaatteisiin. Suojattavat kohteet ja tiedot sekä niiden sijainnit määritellään. Ne luokitellaan julkiseksi, sisäiseksi, luottamukselliseksi tai salaiseksi. Henkilökunnan tietoturvatietämystä selvitetään kyselyllä.

Tietoturvakartoituksen tuloksista käy ilmi tietoturvan huono tilanne organisaatiossa. Tilanteen korjaamiseksi on useita ratkaisuja. Lopuksi tarkastellaan projektin tuloksia puolen vuoden kuluttua.

ASIASANAT:

tietoturva, hallinnollinen tietoturva, tietoturvakartoitus, tietoturvaselvitys

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Information Systems

April 2011 | 39 pages

Instructor: Tuomo Helo

Antti Laine

INFORMATION SECURITY INSPECTION AND INCREASING SECURITY LEVEL – ADMINISTRATIVE SECURITY IN A SMALL ORGANIZATION

This thesis analyzes conducting an information security inspection and increasing the level of information security in a small organization with primary focus on administrative security. The purpose is to increase the level of information security in Association X and give it the tools to upkeep the level.

The first part is about general information security and then delves deeper into administrative security. Information security policy, continuity plans and risk management are an essential part of administrative security.

The next part focuses on inspecting the level of organization's information security and the good principles. Assets, information and their locations are specified. They are classified as public, internal, confidential or secret. Employees' understanding of information security is researched with a query.

The results of information security inspection reveal the grim state of the level of security in the organization. There are many ways to fix the situation. The results of the project are analyzed after six months.

KEYWORDS:

information security, administrative security, information security inspection, information security management

SISÄLTÖ

SANASTO **5**
1 JOHDANTO **6**
2 TIETOTURVA **8**
2.1 Tiedon luottamuksellisuus 9
2.2 Tiedon eheys 9
2.3 Tiedon saatavuus 10
2.4 Todennus, tunnistus ja kiistämättömyys 10
2.5 Hallinnollinen tietoturva 11
2.5.1Tietoturvapolitiikka 13
2.5.2Toipumissuunnitelma ja riskienhallinta 13
3 TIETOTURVAKARTOITUS **15**
3.1 Suojattavat kohteet 16
3.2 Tiedon luokittelu 18
3.3 Tarvittava tietoturvataso 19
3.4 Puutteiden ja riskien määrittely 21
3.4.1Ohjelmistoturvallisuus 21
3.4.2Henkilöstöturvallisuus 23
3.4.3Laiteturvallisuus 27
3.4.4Verkkoturvallisuus 28
3.4.5Varmuuskopiointi 28
4 TIETOTURVATASON NOSTAMINEN **30**
4.1 Ohjelmistojen päivitys 30
4.2 Tietoturvakoulutus 31
4.3 Ohjeistus ja säännöt 32
4.4 Luottamuksellisien tietojen suojaus ja hävittäminen 34
4.5 Toipumissuunnitelma 36
5 TULOSTEN TARKASTELU **37**
5.1 Tulokset 37
5.2 Jatkotoimenpiteet 38
6 LOPPUSANAT **39**
LÄHTEET **40**

LIITTEET

Liite 1. Tietoturvatesti

Liite 2. Windowsin ja muiden ohjelmien päivitykset

Liite 3. Salasana

KUVAT

Kuva 1. PDCA -malli (ISO/IEC 27001 2005). 12
Kuva 2. Näkemykseni hallinnollisesta tietoturvasta 12
Kuva 3. Tietoturvan toteutuminen 21
Kuva 4. Esimerkki tietoturvatestin tuloksista 32

TAULUKOT

Taulukko 1. Tietoturvakartoituksen vaiheet (ISO/IEC 17799 2000, Tietoturvaopas 2010). 15
Taulukko 2. Suojattavien kohteiden jaottelu (ISO/IEC 27002; ISO/IEC 17799 2000). 17
Taulukko 3. Suojattavat tiedot ja niiden sijainnit sekä pääsy niihin. 18
Taulukko 4. Luokittelu. Paljastumisen seuraus (Tietoturvaopas 2010). 19
Taulukko 5. Luokittelu. Oikeus tietoon (Tietoturvaopas 2010). 19
Taulukko 6. Tietoturvakyselyn tuloksia 24
Taulukko 7. Lisää tietoturvakyselyn tuloksia 25
Taulukko 8. Tietoturvakysely, toipumissuunnitelma 25
Taulukko 9. Tietoturvakysely, salasanatietoutta 26
Taulukko 10. Esimerkkejä tietoturvatestin kysymyksistä 32

SANASTO

Konfigurointi	Sovelluksen asetuksien asettaminen. Tuotteen tai palvelun yksilöinti
HTML	Lyhenne sanoista Hypertext Markup Language. Kuvauskieli, jolla Internet-sivut usein ohjelmoidaan
Päällekirjoitus	Laitteella olevan tiedon päälle laitetaan uutta, usein merkityksetöntä tietoa, hävittäen vanhan kokonaan
Salaus	Laitteella oleva tieto muunnetaan ymmärtämättömäksi salasanaa käyttäen. Vain salasanalla voi palauttaa tiedon ymmärrettäväksi

1 JOHDANTO

Opinnäytetyö on osa projektia, jonka tarkoituksena on parantaa pienorganisaation tietoturvan tasoa ja antaa organisaatiolle pohja ylläpitää saavutettua tietoturvatasoa ja nostaa sitä lisää. Työn tavoitteena oli selvittää organisaation tietoturvan sen hetkinen taso, määritella riskit sekä puutteet ja pohtia mahdollisia parannusehdotuksia. Nämä piti esittää ymmärrettävällä tavalla organisaation henkilökunnalle. Tarkoituksena oli antaa organisaatiolle tietoturvaymmärrystä ja saada heidät ajattelemaan asiaa. Tämä voi auttaa organisaatiota tietoturvan ylläpidossa tulevaisuudessa.

Työn aiheena oli aluksi ”Tietoturva pienorganisaatiossa”. Koska tietoturva on todella laaja aihe, päätin rajata aihetta organisaation tarpeiden mukaan, jotta se sopi laajuudeltaan paremmin opinnäytetyöksi. Lopulliseksi aiheeksi muodostui ”Tietoturvakartoitus ja tietoturvatason nostaminen. Hallinnollinen tietoturva pienorganisaatiossa”. Käytännön työhön kuului hallinnollisen tietoturvan lisäksi muitakin tietoturvan osa-alueita, joita myös käsittelen lyhyesti.

Toimeksiantajana toimii Yhdistys X, jonka oikeaa nimeä ei mainita tietoturvasyistä. Yhdistyksen henkilökuntaan kuuluu 10-20 henkilöä. Olin kyseisessä yhdistyksessä harjoittelijana ja tutustuttuani organisaation toimintaan, huomasin useita puutteita sen tietoturvassa. Johdon kanssa keskusteltuani tulimme tulokseen, että tietoturva olisi mainio opinnäytetyön aihe. Olin jo aikaisemmin kiinnostunut tietoturvasta ja sen merkitys on nykymaaillmassa suuri. Tulevaisuudessa se tulee olemaan vieläkin tärkeämpää tietotekniikan kehittyessä.

Tutkimusraportin teoriaosuudessa kerron lyhyesti ja yleisesti tietoturvasta ja sen merkityksestä, jonka jälkeen käsittelen tarkemmin hallinnollista tietoturvaa ja siihen liittyviä asioita, kuten tietoturvapolitiikka, riskianalyysi, riskienhallinta ja toipumissuunnitelma. Tämän jälkeen käsittelen tietoturvakartoituksen tekemistä ja kuvailen suorittamaani kartoitusta. Kerron myös, miksi päädyin valitsemiini ratkaisuihin. Käsittelen toimia, joita suoritin parantaakseni tietoturvan tasoa

Yhdistys X:ssä. Lopuksi pohdin projektin tuloksia puolen vuoden kuluttua sen toteutuksesta.

2 TIETOTURVA

Tietoturvalla tarkoitetaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tietoturvaan liitetään usein myös kiistämättömyys, tunnistus ja todennus. Käsittelen näitä tietoturvan osia alaluvuissa. (Calder 2005, 11.)

Tietoturva on alati uutisten otsikoissa. Välillä haittaohjelma leviää vauhdilla, joskus taas jokin yritys hukkaa asiakkaidensa luottamuksellisia tietoja. Tietoturvan tärkeys niin organisaatioille kuin yksityisille henkilöillekin kasvaa. Tietokoneille tallennetaan aikaisempaa enemmän informaatiota ja suuri osa siitä kulkee Internetissä. Tämä kasvattaa tietoturvasovellusten vaatimuksia ja yksilöiltä vaaditaan yhä enemmän osaamista ja ymmärrystä, etenkin tietoturvan alueelta. Teknologian kehittyessä vaatimukset tulevat nousemaan entisestään ja tietoturvaonnettomuudet yleistyvät.

Tietoturvaonnettomuudet voivat aiheuttaa organisaatiolle monenlaisia hankaluuksia. Ne voivat hidastaa tai pysäyttää organisaation tärkeitä toimintoja, joita ilman se ei tule toimeen. Puutteet toiminnoissa voivat aiheuttaa rahallisia menetyksiä ja niiden korjaaminen voi maksaa lisää. Joissain tapauksissa organisaatio voi olla velvollinen korvaamaan aiheutuneet haitat sen asiakkaille. Organisaatio voi myös menettää maineensa ja siten asiakkaidensa luottamuksen, joka johtaa taas rahallisiin menetyksiin. Huonosta tietoturvasta johtuvat tietoturvaonnettomuudet voivat johtaa oikeudellisiin toimenpiteisiin, joiden selvittämiseen menee rahaa. Voi siis sanoa, että huono tietoturva kasvattaa tietoturvaonnettomuuden uhkaa ja sen aiheuttamaa riskiä. Tämän vuoksi riski menettää rahaa ja menetyksen suuruus kasvavat. Tietoturvaan kannattaa siis sijoittaa rahaa, koska puutteellinen tietoturva voi tulla vielä kalliimmaksi.

Ei ole olemassa täydellistä tietoturvatuotetta, joka takaisi täydellisen tietoturvan. Täydellistä tietoturvaa ei ole olemassakaan. Tietoturvan tehtävänä onkin hallita riskejä eikä poistaa niitä kokonaan. Tietoturva auttaa varautumaan riskeihin ja siten toipumaan onnettomuuksista nopeammin ja paremmin. Tietoturvan taso

on parhaimmillaan kun tietoturvasovellukset yhdistetään hyvään tietoturvan hallintaan. (Microsoft TechNet 2010.)

2.1 Tiedon luottamuksellisuus

Tiedon luottamuksellisuus tarkoittaa, että tieto on saatavilla vain sellaisille henkilöille, järjestelmille tai prosesseille, joilla on oikeus kyseiseen tietoon. Sitä ei paljasteta muille. Luottamuksellista tietoa voivat olla esimerkiksi henkilötunnus, sairaskertomus, luottokortin numero ja organisaation transaktiotiedot. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Luottamuksellisuutta voidaan yrittää taata esimerkiksi salassapitosopimuksilla, jolloin sopimuksen allekirjoittaneet sidotaan lailla sen säilyttämiseen. Tietoa voi myös salata erilaisilla menetelmillä, jolloin ulkopuolisten on hankala päästä siihen käsiksi. Tietoon oikeutetuista henkilöistä pidetään listaa ja heille annetaan tunnukset, joilla he pääsevät käsiksi tietoon. Käyttäjien toimia täytyy valvoa järjestelmässä. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

2.2 Tiedon eheys

Tiedon eheys tarkoittaa, että tieto ei ole virheellistä. Virheellisyydellä ei tarkoiteta sen paikkansapitävyyttä, vaan sitä, ettei se ole vahingoittunut. Tietojärjestelmän virhe tai haittaohjelma saattaisi aiheuttaa muutoksia tiedossa, jolloin se olisi virheellistä. Myös luvattomat ja vahingolliset muutokset vaikuttavat tiedon eheyteen. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Tiedon eheyttä voidaan varmistaa tekemällä säännöllisesti varmuuskopioita. Tiedon muuttuminen pitää voida huomata ja jäljittää, jotta varmuuskopioista olisi hyötyä. Virustorjuntaohjelmat ja tietoturvakoulutus vähentävät tiedon eheyden menettämisen riskiä. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

2.3 Tiedon saatavuus

Tiedon saatavuus tai käytettävyys tarkoittaa, että tieto on saatavilla ja käytettävissä, kun sitä tarvitaan. Saatavuutta uhkaavat esimerkiksi tietojen tuhoutuminen tai katoaminen, tietojärjestelmien ja laitteiden toimimattomuus sekä yhteyksien katkeaminen. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Hyvän saatavuuden varmistamiseksi järjestelmiä ja fyysisiä laitteita pitää huoltaa säännöllisesti, tarpeen mukaan, jolloin niiden toimimattomuuden riski vähenee. Tietojen tuhoutuessa toimivat ja säännölliset varmuuskopiot auttavat palauttamaan saatavuuden. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

2.4 Todennus, tunnistus ja kiistämättömyys

Luottamuksellisuuden ja eheyden takaamiseen kuuluu todennus ja tunnistus. Todennuksella tarkoitetaan käyttäjän todennusta eli järjestelmä varmistaa, että sen käyttäjä on jokin tietty henkilö, jolla on oikeus käyttää sitä ja päästä käsiksi tietoihin. Se voidaan toteuttaa käyttämällä käyttäjätunnusta ja salasanaa, jolloin vain oikeutettu taho, joka tietää niiden yhdistelmän, pääsee käyttämään järjestelmää. Monimutkaisemmissa järjestelmissä voidaan lisäksi käyttää esimerkiksi tietokoneen laitteiston tunnistusta, jolloin vain tietyiltä laitteilta pääsee käyttämään järjestelmää. Tunnistus tarkoittaa, että käyttäjätunnus voidaan yhdistää johonkin henkilöön, järjestelmään tai prosessiin. (Raggad 2009.)

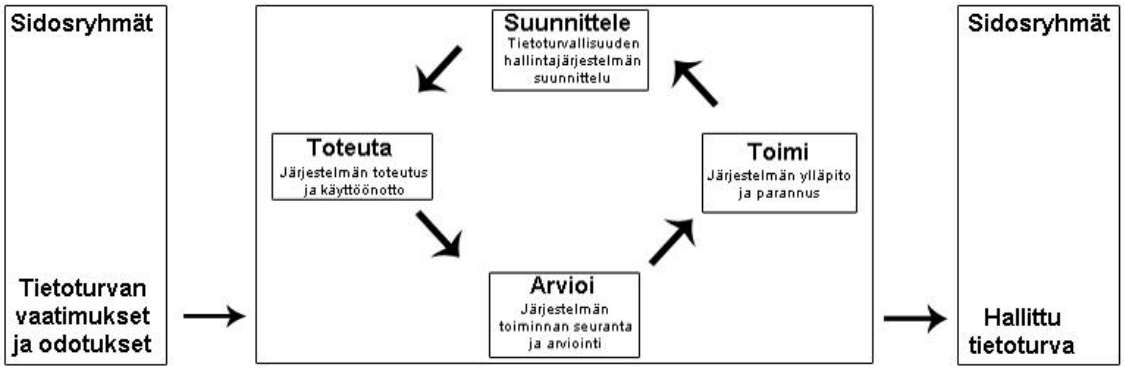
Kiistämättömyys tarkoittaa, että todennettu ja tunnistettu henkilö ei voi kiistää suorittamiaan toimia järjestelmässä. Kaikki hänen tekemänsä toimet ja muutokset tallentuvat järjestelmään. On myös mahdollista käyttää digitaalisia allekirjoituksia. Ne muodostetaan alkuperäisen tiedon mukaan. Jos tietoa muutetaan tai jos se muuttuu jostain muusta syystä, digitaalinen allekirjoitus ei enää vastaa uutta tietoa, jolloin järjestelmä tietää, että tieto on muuttunut. (Caelli & McCullagh 2000.)

2.5 Hallinnollinen tietoturva

Organisaation hallinnon täytyy vähintään pitää huolta, ettei organisaation toiminta ole lainvastaista. Hyvän tietoturvan kannalta on kuitenkin tärkeää, että organisaation hallinto on sitoutunut noudattamaan, ylläpitämään ja päivittämään tietoturvapolitiikkaa. Sen pitää ymmärtää tietoturvan tärkeys. Jos hallinto ei ole lainkaan kiinnostunut tietoturvasta, on todennäköistä, etteivät he ylläpidä tietoturvan tasoa ja henkilöstön tietoturvaosaamista. Hallinnon pitää huomata uhat ja riskit. (Calder & Watkins 2005, 13.)

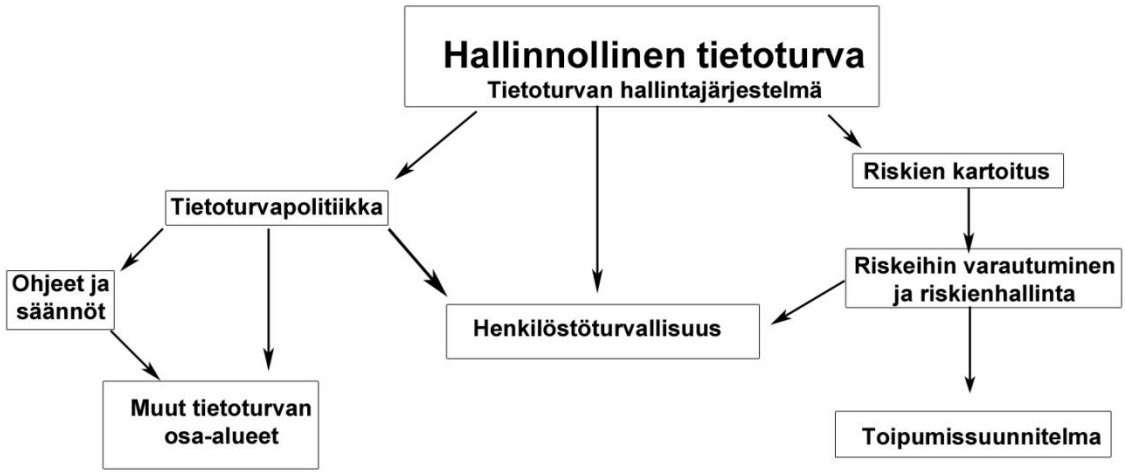
Henkilöstön tietoturvaosaamisen ylläpito onkin yksi tietoturvan hallinan tärkeimmistä tehtävistä. Tietoturvaa ymmärtävä henkilökunta on huomattavasti pienempi riskitekijä kuin sitä ymmärtämätön henkilökunta. Henkilökunnan koulutus voi myös olla halvempaa kuin monet muut menetelmät. Tärkeintä on, että henkilökunta tiedostaa olemassa olevat riskit. (Maiwald 2002, 118.)

Organisaatiossa täytyy nimittää ainakin yksi henkilö, joka vastaa tietoturvan hallinnasta. Hänen ei tarvitse tietää kaikkea tietoturvasta, mutta jonkinlainen tietoturvaymmärrys hänellä täytyy silti olla. Hän voi muodostaa organisaation sisäisen tietoturvakeskusteluryhmän, joka kokoontuu keskustelemaan organisaation tietoturvasta tietyn aikavälein. Hän pitää huolta, että tämänhetkiset uhat ovat keskusteluryhmän tietoisuudessa. Keskusteluryhmässä voidaan pohtia, kuinka uhkiin voidaan varautua. Tietoturvan hallinnoijan tehtäviin kuuluu myös tietoturvaonnettomuuksien ylöskirjaaminen. (Calder & Watkins 2005, 52-53.)



Kuva 1. PDCA -malli (ISO/IEC 27001 2005).

Kuva 1 esittää tietoturvallisuuden hallintajärjestelmän, sidosryhmien ja prosessien välisiä vuorovaikutuksia PDCA –mallin (Plan-Do-Check-Act) mukaisesti. Sidosryhmät, kuten asiakkaat ja yhteistyökumppanit, saattavat vaatia organisaatiolta tietoturvallisia menettelytapoja. Ensin tietoturvan hallinta suunnitellaan, johon kuuluu tietoturvapolitiikan, tavoitteiden, prosessien ja menettelytapojen määrittely. Tämän jälkeen se toteutetaan ja otetaan käyttöön. Hallinnan toimivuutta arvioidaan koko ajan ja sen toimintaa verrataan tavoitteisiin. Toimintavaiheessa mahdolliset puutteet korjataan ja suoritetaan lisäykset. Parannukset suunnitellaan ja toteutetaan. Tuloksena on paremmin hallinnassa oleva tietoturva. (ISO/IEC 27001 2005.)



Kuva 2. Näkemykseni hallinnollisesta tietoturvasta

Hallinnollinen tietoturvaa voisi pitää tärkeimpänä tietoturvan osa-alueena. Jos hallinnollinen tietoturva toimii organisaatiossa hyvin, se ylläpitää muita tietoturvan alueita. Se on tietoturvan hallintaa, tietoturvan johtamista. Siihen kuluu sopimuksia, suunnitelmia ja yhteistyötä. Kuvassa 2 on näkemykseni hallinnollisesta tietoturvasta. Tietoturvapolitiikkaa käytetään hyväksi sääntöjen ja ohjeiden luomisessa sekä muiden tietoturvan osa-alueiden hallinnassa. Hallinnollinen tietoturva vaikuttaa henkilöstöturvallisuuteen sekä suoraan, että tietoturvapolitiikan kautta. Myös riskeihin varautuminen ja niiden hallinta vaikuttavat siihen.

2.5.1 Tietoturvapolitiikka

Tietoturvapolitiikka sisältää päätettyjä toimintatapoja tietoturvan edistämiseksi. Se ei aina kerro täsmälleen, mitä tehdään, vaan se voi olla ennemminkin suuntaa antava ja siinä määritellään organisaation tietoturvan tavoitteet strategisella tasolla. Sitä kannattaa käyttää pohjana säännöille, ohjeille ja suosituksille. Se on kirjoitettu selkeällä kielellä ja sen ymmärtäminen ei vaadi erityistä teknistä tai muunlaista osaamista. Tietoturvapolitiikkaa pitää päivittää ja ylläpitää organisaation tarpeiden ja tilanteen muuttuessa. (Baskerville ym. 2008, 124-126.)

2.5.2 Toipumissuunnitelma ja riskienhallinta

Toipumissuunnitelma on dokumentti tai kokoelma dokumentteja, jossa käsitellään tietoturvaonnettomuuksista selviämistä. Toipumissuunnitelmaa luodessa on mietittävä, mitä organisaatiolle tärkeitä toimintoja organisaatiolla on. Näitä voivat olla esimerkiksi palkanmaksu, asiakkaiden palvelu ja tuotteiden myynti. Tämän jälkeen on arvioitava, kuinka pitkä eri toimintojen toimimattomuus saa enintään olla, ennen kuin siitä aiheutuu liian suurta haittaa organisaatiolle. On myös huomioitava, paljonko tietoa saa kadota ennen kuin siitä aiheutuu huomattavia ongelmia. (Gregory 2008, 18–20.)

Jos pieni organisaatio menettää päivän aikana keräämänsä tiedot, siitä voi tilanteesta ja organisaatiosta riippuen olla vain vähän haittaa, koska tiedot voidaan kerätä uudestaan. Sen aiheuttama lisätyö ei välttämättä kaada koko organisaatiota. Jos pieni organisaatio menettäisi kaikki keräämänsä tiedot puolen vuoden ajalta, niiden takaisin kerääminen saattaisi olla mahdotonta. Jos tiedot olisivat välttämättömiä organisaation toiminnalle, se olisi suurissa ongelmissa.

Toipumissuunnitelmaan kuuluu yleensä riskianalyysi. Siinä määritellään jokaiselle organisaation tärkeälle toiminnolle tai tiedolle niihin liittyviä tietoturvaonnettomuuksia, jotka voisivat toteutua. Kannattaa käyttää useita erilaisia menetelmiä riskien löytämiseksi. Ei ole kuitenkaan järkevää listata tietoturvaonnettomuuksia, joiden toteutuminen on todella epätodennäköistä. Arvioitu todennäköisyys onnettomuuksien toteutumiselle kannattaa merkitä ylös. Jos on hyvin todennäköistä, että uhka toteutuu, on järkevää priorisoida kyseisen riskin käsittely ensimmäiseksi. (Gregory 2008, 20; VTT 2009.)

Riskianalyysissä kannattaa alussa keskittyä yhteen kohteeseen eli toimintoon kerrallaan. On tärkeää, että ainakin yksi toimintoon liittyvä henkilö on mukana analyysin tekemisessä. Hän tuntee työnsä ja pystyy siksi kertomaan siitä. (VTT 2009.)

Kun riskit on kartoitettu, pitää kehittää suunnitelmat niiden hallitsemiseksi. Riskienhallintaan sisältyy riskien poistamista, riskien vähentämistä ja riskien siirtämistä. Tietojen varmuuskopioiminen kunnollisella tavalla poistaa käytännössä suuren luokan tietojen menetyksen riskin. Hyvän tietoturvasovelluksen käyttöönotto vähentää huomattavasti haittaohjelmien aiheuttamaa riskiä, muttei kuitenkaan poista sitä kokonaan. Riskien siirtäminen voi tarkoittaa esimerkiksi vaakuutuksien ottamista, jolloin rahallinen riski siirretään vakuutusyhtiölle. (Calder & Watkins 2005, 80.)

3 TIETOTURVAKARTOITUS

Hyvän tietoturvakartoituksen pohjana on toimiva yhteystyö. Yhteistyössä toimivat tietoturvan asiantuntija(t), tutkittavan alueen tai kohteen tuntija(t) ja organisaation päättäjät. Tietojärjestelmän kehittäjät ja käyttäjät tuntevat parhaiten sen käytön ja toiminnan. Ulkopuoliset asiantuntijat saattavat huomata ongelmat helpommin kuin tavalliset jäjestelmän käyttäjät. (VTT 2009.)

Tietoturvakartoituksessa kannattaa keskittyä yhteen rajattuun kohteeseen kerrallaan ja käyttää useita menetelmiä riskien löytämiseksi. Riskejä käsitellessä täytyy käyttää järkeä. Mitättömään ja merkityksettömään riskiin keskittyminen olisi ajan ja resurssien tuhlausta. (VTT 2009.)

Tietoturvakartoitukseen kuuluu suojattavien kohteiden määrittely, selvittäminen ja luokittelu, riskien määrittely ja analysointi, sekä puutteiden listaaminen. Taulukossa 1 kuvattavia tietoturvakartoituksen vaiheita käsitellään tarkemmin myöhemmin. Jotta tietoturvakartoituksen voi tehdä kunnolla, on ensin ymmärrettävä, mitä tieto ja tietoturva tarkoittavat. On myös järkevää määritellä tavoitetaso tietoturvalle, jotta nykytilaa voi verrata siihen. (ISO/IEC 17799 2000.)

Taulukko 1. Tietoturvakartoituksen vaiheet (ISO/IEC 17799 2000, Tietoturvaopas 2010).

Vaihe	**Kuvaus**
Suojattavien kohteiden määrittely	Toiminnalle tärkeät tiedot, laitteet yms.
Suojattavien kohteiden selvittäminen	Missä kohteet sijaitsevat, kuka niitä käyttää
Suojattavien kohteiden luokittelu	Kohteiden tärkeys organisaation toiminnalle
Riskien määrittely	Kohteisiin liittyvät riskit
Riskien analysointi	Riskien oteutumisen todennäköisyys, haitan suuruus
Puutteiden määrittely	Mitkä riskit ovat liian vakavia verrattuna tavoitetasoon

Ollessani harjoittelemassa Yhdistys X:ssä, huomasin organisaation toimintoihin tutustuessani vakavia puutteita organisaation tietoturvassa. Henkilöstön ja johdon tietoturvatietoisuus vaikutti hyvin vähäiseltä. Yhdistys tarvitsi paremman tietoturvatason, muttei voinut maksaa kalliista, yritysten tarjoamista, standardeja noudattavista, tietoturvaratkaisuista. Asiasta oli keskusteltu hieman harjoittelun alussa ja lopussa sovimme, että teen aiheesta opinnäytetyön.

Tutustuessani erilaisiin tietoturvamateriaaleihin, huomasin, että suurin osa niistä oli tarkoitettu suuremmille organisaatioille. Pienet organisaatiot eivät voi muodostaa valtavia tietoturvaprojekteja, joiden parissa useat henkilöt työskentelelisivät pitkällä aikavälillä.

3.1 Suojattavat kohteet

Suojattaviin kohteisiin kuuluu kaikki organisaation toiminnalle tärkeät tiedot ja asiat tai niitä sisältävät kohteet. Suojattavat kohteet voidaan jaotella henkilöihin, laitteisiin, tiloihin, palveluihin, tietoaineistoihin ja tietojärjestelmiin. Henkilöihin voivat kuulua ne, joita tarvitaan organisaation päivittäisen toiminnan ylläpitämisessä. Laitteisiin kuuluvat esimerkiksi palvelimet, työasemat ja puhelimet. Palveluilla tarkoitetaan organisaation tuottamia palveluita, joiden toimimattomuus saattaisi aiheuttaa organisaatiolle huomattavia kustannuksia. Tietojärjestelmiin sisältyy esimerkiksi tietokannat ja rekisterit, ja tietoaineistoihin sisältyy paperit, USB-muistitikut ja muut tallennusmediat. Suojattavat kohteet voidaan myös jaotella, kuten taulukossa 2. Ohjelmistojen ongelmat vaikuttavat suoraan tietoon, fyysiset kohteet vaikuttavat joko suoraan tietoon tai ohjelmistojen kautta. Työntekijät ovat tietenkin tärkeitä ja ongelmat palveluissa vaikuttavat laitteiden ja työntekijöiden toimintaan. Maine voi olla hyvinkin tärkeä organisaatiolle. Maineensa menettänyt organisaatio menettää myös asiakkaidensa luottamuksen ja siten mahdollisesti asiakkaansa. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Taulukko 2. Suojattavien kohteiden jaottelu (ISO/IEC 27002; ISO/IEC 17799 2000).

	Kuvaus
Tieto	Tietokannat, tiedostot, sopimukset, asiakirjat, ohjeistukset, suunnitelmat, arkistoidut tiedot
Ohjelmistot	Apuohjelmat, kehitystyökalut, sovellusohjelmistot ja järjestelmäohjelmistot. Esimerkiksi tietokantasovellus, käyttöjärjestelmä, Microsoft Office.
Fyysiset kohteet	USB-muistit, palvelimet, työasemat, verkko- ja tietoliikennelaitteisto
Palvelut	Sähkö, valaistus, ilmastointi, lämmitys, tietoliikennepalvelut
Ihmiset	Työntekijät ja heidän osaamisensa ja kokemuksensa
Aineetomat asiat	Organisaation maine ja imago

Aloitin suojattavien kohteiden listaamisen selvittämällä, mitkä ovat Yhdistys X:lle tärkeitä resursseja ja tietoja. Muodostin listan kyselemällä henkilökunnalta, mitä tietoja he käyttävät ja tarvitsevat päivittäisessä työssään ja minkä puuttuminen aiheuttaisi ongelmia. Selvitin myös yhdistyksen toimintoja ja kokosin listan suojattavista tietokokonaisuuksista. Esimerkiksi jäsenrekisteri, asiakastietorekisteri, palvelurekisteri, henkilökunnan tiedot, yhdistyksen www-sivut ja keskustelualue, muut asiakkaiden yksityiset tiedot ja yhdistyksen sisäiset tiedot.

Seuraavaksi selvitin, mistä kyseiset tiedot löytyvät. Taulukko 3 havainnollistaa asiaa. Suurin osa tiedoista sijaitsi palvelimella, mutta osa tiedoista löytyi myös pöydiltä USB-muistitikuilta ja papereilta. Osaan tiedosta pääsi liian helposti käsiksi, koska niitä ei oltu suojattu mitenkään.

Taulukko 3. Suojattavat tiedot ja niiden sijainnit sekä pääsy niihin.

Suojattava tieto	Sijainnit	Pääsy tietoon
Jäsenrekisteri	Palvelin, osa tiedoista myös USB-tikuilla, työasemilla ja papereilla	Salasanalla tietyistä työasemista. Osa tiedoista suojaamattomana
Asiakasrekisteri	Palvelin, osa tiedoista myös USB-tikuilla, työasemilla ja papereilla	Salasanalla tietyistä työasemista. Osa tiedoista suojaamattomana
Palvelurekisteri	Palvelin, osa tiedoista myös USB-tikuilla, työasemilla ja papereilla	Salasanalla tietyistä työasemista. Osa tiedoista suojaamattomana
Henkilökunnan tiedot	Palvelin, kassakaapissa olevat paperit	Salasanalla tietyistä työasemista.
Muut asiakkaiden yksityiset tiedot	Työasemat, palvelin, USB-tikut, paperit	Tiedot ovat suojaamattomana
Yhdistyksen sisäiset tiedot	Työasemat, palvelin, paperit	Tiedot ovat suojaamattomana
www-sivut	Ulkoistettu palvelin	Käyttäjätunnus ja salasana, miltä tahansa koneelta
Keskustelualue	Ulkoistettu palvelin	Käyttäjätunnus ja salasana, miltä tahansa koneelta

Päädyin tähän yksinkertaiseen ratkaisuun, koska organisaatio oli hyvin pieni ja sen järjestelmät ja toiminnot eivät olleet monimutkaisia. Näin säästin aikaa ja kokonaisuudesta tuli selkeämpi ja ymmärrettävämpi.

3.2 Tiedon luokittelu

Tiedon luokittelu auttaa yksinkertaistamaan tiedon käsittelyä ja sen suojaamista. Taulukon 4 esimerkki luokittelee tiedot perustuen paljastumisesta aiheutuviin seurauksiin. Julkinen tieto voi olla mitä tahansa tietoa, jota organisaatio voisi vaikka laittaa www-sivuilleen. Sisäinen tieto on organisaation toimintaan liittyvää tietoa, joka ei kuulu ulkopuolisille. Se ei kuitenkaan sisällä luottamuksellista. Luottamuksellinen ja salainen tieto voivat olla esimerkiksi asiakkaan henkilötietoja. Luottamuksellinen ja salainen tieto voivat olla sama asia pienissä organisaatioissa, joissa tietoa ei tarvitse luokitella kovin tarkasti. (Tietoturvaopas 2010.)

Taulukko 4. Luokittelu. Paljastumisen seuraus (Tietoturvaopas 2010).

Luokittelu	**Paljastumisen seuraus**
Julkinen tieto	Hyötyä organisaatiolle
Sisäinen tieto	Ei juurikaan vaikutusta
Luottamuksellinen tieto	Haittaa organisaatiolle
Salainen tieto	Suurta haittaa organisaatiolle

Luokittelun kuuluu kertoa myös se, kuka saa nähdä tiedon. Tarvittaessa asiaa voidaan tarkentaa määrittelemällä lisäksi, kuka saa muokata tai poistaa tietoa. Taulukossa 5 näkyy, kenellä on oikeus eri tavalla luokiteltuihin tietoihin. (Tietoturvaopas 2010.)

Taulukko 5. Luokittelu. Oikeus tietoon (Tietoturvaopas 2010).

Luokittelu	**Oikeus tietoon**
Julkinen	Kenellä tahansa
Sisäinen	Organisaation henkilökunnalla tai esimerkiksi jollain tietyllä osastolla
Luottamuksellinen	Tiedon käyttäjällä ja sen omistajalla (Esimerkiksi virkailija ja asiakas, jonka tietoja käsitellään)
Salainen	Tiedon käyttäjällä ja sen omistajalla (Esimerkiksi virkailija ja asiakas, jonka tietoja käsitellään)

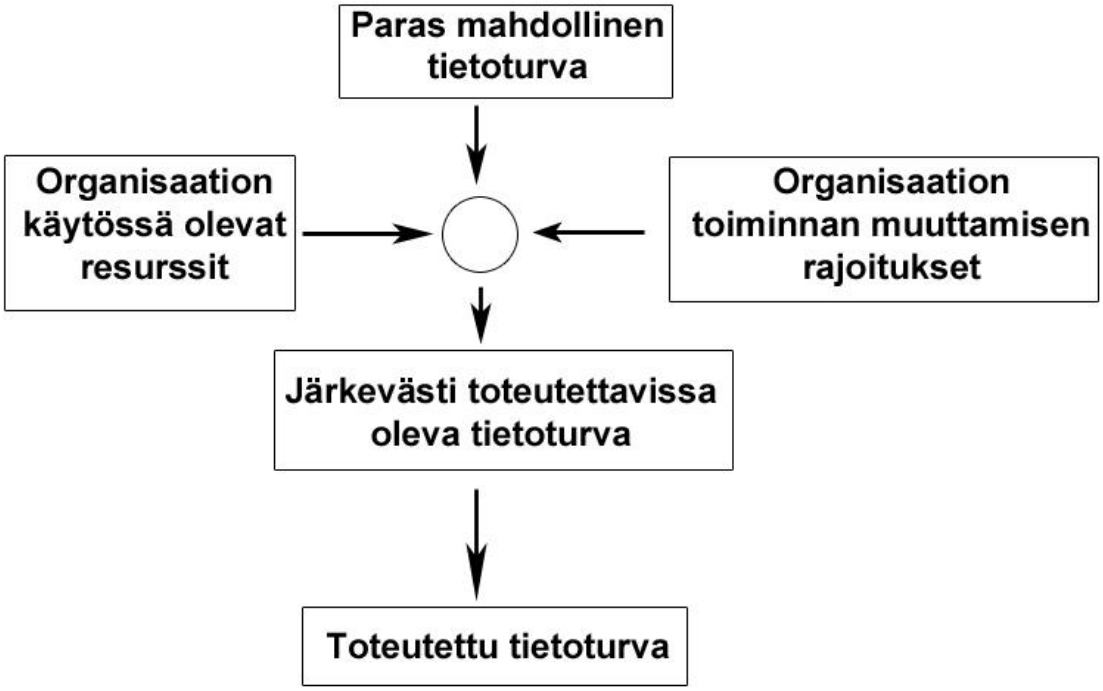
3.3 Tarvittava tietoturvataso

Tarvittavaa tietoturvatasoa voi olla vaikea kuvailla lyhyesti. Se vaihtelee organisaatioittain, riippuen käsiteltävän tiedon tärkeydestä ja

luottamuksellisuudesta. Yhdistys X:n tapauksessa päätimme, että tavoitteena on taso, jossa tietoturvaonnettomuuksien tapahtuminen on epätodennäköistä ja niistä selviäminen on todennäköistä.

Suojattaviin tietoihin liittyvät järjestelmät ja toiminnot eivät saa aiheuttaa riskejä, joiden toteutuminen on todennäköistä. Järjestelmistä pitää olla uusimmat versiot ja tarvittavat suojausasetukset pitää olla käytössä. Henkilökunnan pitää osata ajatella tietoturvallisesti ja tietoturvasäännöt pitää olla olemassa.

Kuvassa 3 käsittelen tietoturvan toteutumista siten, kuin olen kokemuksissani havainnut. Olisi hienoa, jos paras mahdollinen tietoturva voitaisiin aina toteuttaa. Näin ei käytännössä kuitenkaan koskaan ole, etenkään pienissä organisaatioissa. Tietoturvan ylläpitäminen ja toteutus voi vaatia paljon resursseja, enemmän kuin organisaatiolla on varaa käyttää tietoturvaan. Sen toteuttaminen voisi myös vaatia huomattavia muutoksia organisaation toimintaan. Kaikkea ei välttämättä voida tai haluta muuttaa. Muutosprosessi voisi myös vaatia lisää resursseja. Sitten päädytään järkevästi toteutettavissa olevaan tavoiteratkaisuun. Sen perusteella toteutettu tietoturvaratkaisu on saattaa poiketa tavoitteesta, kun toteutuksen aikana huomataan lisää ongelmia resurssien ja toimintojen muuttamisen kanssa.



Kuva 3. Tietoturvan toteutuminen

3.4 Puutteiden ja riskien määrittely

Kun suojattavat tiedot on selvitetty ja luokiteltu, ja tarvittava tietoturvataso on määritelty, aletaan selvittämään tarkemmin tietoturvan nykytilan puutteita. Käsittelen seuraavaksi ohjelmistoihin liittyvää tietoturvaa ja määrittelen niiden puutteet. Sitten käsittelen henkilöstöturvallisuutta, laiteturvallisuutta ja tietojen varmuuskopioimista.

3.4.1 Ohjelmistoturvallisuus

Ohjelmistoissa olevat suunnittelu- ja ohjelmointivirheet saattavat aiheuttaa tiedon katoamista tai muuttumista. Ne voivat myös mahdollistaa ulkopuolisen henkilön tai sovelluksen pääsyn tietoon. Riskiä voidaan vähentää päivittämällä ohjelmistoja säännöllisesti. Joskus voi olla tarpeen vaihtaa ohjelmisto toiseen.

Väärin konfiguroidut asetukset voivat aiheuttaa samanlaisia ongelmia. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Työasemilla ei pitäisi olla tarpeettomia sovelluksia asennettuna. Tarpeellisten sovellusten mahdolliset tietoturvaan liittyvät asetukset täytyy asettaa siten, että vain tarpeelliset toiminnon toimivat. Jos organisaatiolla on heille kustomoituja sovelluksia, on otettava selvää, onko ne testattu tietoturva-aukkojen varalta. (Hayes 2003.)

Kun aloitin ohjelmistojen tutkimisen Yhdistys X:ssä, ensimmäiset asiat jotka minulle tulivat mieleen, olivat ajan tasalla olevat virustorjunta- ja palomuuriohjelmistot. Yhdistys X:ssä oli käytössä Symantecin yhdistetty virustorjunta ja palomuuri. AV-Comparatives.org sivuston mukaan Symantecilla on melko hyvä maine ja se sai testeissä ADVANCED+ arvosanan, joka on paras mahdollinen arvosana. Symantecin virustentunnistusprosentti ollut paras vaihtoehdoista, mutta se oli kuitenkin kilpailukykyinen (AV-Comparatives.org 2010). Ohjelmiston asetuksia en voinut tarkastella tarkasti, mutta huomasin, että käyttäjä voi asettaa suojaukset pois päältä. Joissakin tietokoneissa, etenkin kannettavissa, ohjelmistoa ei ollut päivitetty. Tämä oli hieman huolestuttavaa, koska automaattiset päivitykset olivat päällä. Selvityksen jälkeen tulin siihen tulokseen, että päivitykset oli ajoitettu huonosti joidenkin työntekijöiden aikatauluun verrattuna. Tämän vuoksi uusimmat haittaohjelmat jäävät todennäköisesti virustorjuntaohjelmalta huomaamatta. Haittaohjelmat saattavat hidastaa tietokonetta ja verkkoa, ja siten hidastaen myös työntekoa. Ne voivat myös tuhota, sotkea ja varastaa tietoa. Pahimmassa tapauksessa haittaohjelma levittää itseään tai lähettää roskapostia käyttäen Yhdistys X:n tietokoneita.

Käyttöjärjestelmien päivityksistä löytyi myös puutteita. Ongelma oli taas suurin kannettavissa tietokoneissa. Käyttöjärjestelmänä käytettiin Windows XP:tä. Microsoft lopettaa kaiken tuotetuen ja päivitykset 8.4.2014. Windows XP on siis vanhentunut käyttöjärjestelmä ja tietoturvapäivitysten lakatessa haittaohjelmat ja rikolliset voivat hyödyntää järjestelmässä olevia heikkouksia, aiheuttaen vakavia ongelmia, kuten tietojen menetystä (Microsoft 2010.)

Microsoft Officen ja muiden käytössä olevien hyötyohjelmien mahdollisia tietoturvapuutteita en voinut tarkastella paljonkaan, mutta on aina hyvä muistaa, että Internetistä ladatut tiedostot saattavat sisältää haittaohjelmia. Microsoft Access tietokantasovelluksen makrot oli sallittu, joka mahdollistaa haitallisen koodin ajamisen tietokoneissa, jos tietokanta on saastunut haittaohjelmalla tai sen tekijä on tarkoituksella niin tehnyt. Tämä oli kuitenkin pakollista, koska luotettujen sijaintien määrittely ohjelman asetuksissa ei aina toiminut. Luotettavien sijaintien määrittelyn pitäisi mahdollistaa koodin ajamisen niissä tapauksissa, joissa tietokanta sijaitsee määritellyissä sijainneissa. Päättelin kuitenkin, että riski on pieni, koska kukaan Yhdistys X:ssä ei lataa Internetistä tietokantoja koneille. Sille ei yksinkertaisesti ole minkäänlaista hyvää tai huonoa syytä.

3.4.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella yritetään ehkäistä henkilökunnan aiheuttamia tietoturvauhkia. Organisaatio voi parantaa henkilöstöturvallisuutta varmistamalla ennen henkilöiden työsuhteiden alkua, että he ovat luotettavia ja heidän osaamisensa on riittävän hyvä. Heidän koulutustaustansa, henkilöllisyytensä ja mahdolliset rikostaustat täytyy tarkistaa. Heidän täytyy myös ymmärtää omat velvollisuutensa. Velvollisuudet täytyy tehdä selväksi työsopimuksella, joka heidän täytyy hyväksyä. Työsopimuksen lisäksi voi olla henkilötietolakiin liittyviä salassapitosopimuksia, jos työntekijä käsittelee henkilötietoja. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Työsuhteen aikana organisaation hallinnon täytyy edellyttää henkilökunnalta sääntöjen, ohjeiden ja muiden velvollisuuksien noudattamista. Ohjeet ja säännöt täytyy olla helposti kaikkien saatavilla ja jokaisen pitää ymmärtää, että niitä pitää noudattaa. Heidän täytyy myös valvoa niiden noudattamista, koska muulloin niitä ei välttämättä kuitenkaan noudateta. Tarpeen vaatiessa henkilökuntaa täytyy rangaista velvollisuuksiensa laiminlyönneistä. Rankaisun lisäksi hallinnon kannattaa muutenkin motivoida henkilökuntaa noudattamaan

tietoturvasääntöjä, esimerkiksi keskustelemalla asiasta usein. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Henkilökunnalle täytyy antaa jonkinnäköinen tietoturvakoulutus tai muuten varmistaa, että heidän tietoturvaymmärryksensä on riittävä. Vaadittavan tietoturvaymmärryksen määrä riippuu henkilön roolista organisaatiossa. Henkilötietoja käsittelevä henkilö tarvitsee todennäköisesti paremman ymmärryksen kuin varastolla laatikoita kantava työntekijä. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Työsuhteiden päättymisen jälkeen on varmistettava, että kaikki organisaation omaisuus, kuten kannettavat, puhelimet ja usb-muistit palautetaan. On myös pidettävä huolta, että kaikki heidän käyttäjätunnuksensa otetaan pois käytöstä. Jos työsuhde päättyy riitaisissa merkeissä, täytyy varoa mahdollisia kostotoimenpiteitä, kuten tietojen sotkemista tai varastamista. (ISO/IEC 27002; ISO/IEC 17799 2000.)

Ihminen on siis suuri riskitekijä tietoturvassa. Tämän vuoksi halusin tietää, mitä henkilökunta tietää ja ajattelee tietoturvasta. Valmistin lyhyen kyselyn, joka tallentaa vastaukset nimettömänä tietokantaan. Kokosin tiedot yhteen ja tein asiasta havaintoja. Taulukoissa ylin arvo tarkoittaa suurinta annettua arvoa ja alin pienintä annettua arvoa. Kyselyyn vastasi koko henkilökunta.

Taulukko 6. Tietoturvakyselyn tuloksia

	Salasanan tietoturva tietoisuus	Salasanan tietoturva tärkeys	Kannettavan tietoturva tietoisuus	Kannettavan tietoturva tärkeys	Muistitikun tietoturva tietoisuus	Muistitikun tietoturva tärkeys
Ylin	10	10	10	10	10	10
Keskiarvo	6,7	9,2	5,3	8,5	4,2	8,6
Alin	2	6	1	1	1	3

Kuten taulukosta 6 käy ilmi, osa henkilökunnasta ei uskonut tietävänsä muistitikkuihin, kannettaviin tietokoneisiin tai salasanoihin liittyvästä tietoturvasta juuri mitään. Huolestuttavinta oli, että osa henkilökunnasa ei

pitänyt asioita kovinkaan tärkeinä. Tämä kertoo siitä, että he eivät tienneet tai ymmärtäneet tietoturvariskejä. Keskimäärin oman tietoisuuden uskottiin olevan keskinkertaista ja asioiden tärkeyttä pidettiin korkeana.

Taulukko 7. Lisää tietoturvakyselyn tuloksia

	Sähköpostin tietoturva tietoisuus	Sähköpostin tietoturva tärkeys	Yleinen tietoturva tietoisuus	Yleinen tietoturva tärkeys	Käyttöoikeudet tietoisuus	Käyttöoikeudet tärkeys
Ylin	10	10	9	10	9	10
Keskiarvo	6,1	9,1	6,5	9,4	6,4	9,3
Alin	1	3	3	6	3	7

Taulukossa 7 näkyvät tulokset ovat hyvin samankaltaisia kuin taulukossa 6 näkyvät tulokset. Yleistä tietoturvaa ja käyttöoikeuksia pidettiin hyvin tärkeinä ja alimmat arvotkin olivat melko korkeat.

Taulukko 8. Tietoturvakysely, toipumissuunnitelma

	Toipumissuunnitelma tietoisuus	Toipumissuunnitelma tärkeys
Ylin	10	10
Keskiarvo	3,8	8,5
Alin	1	6

Keskimäärin toipumissuunnitelmasta uskottiin tietävän hyvin vähän, kuten taulukosta 8 näkee. Asiaa pidettiin kuitenkin tärkeänä. Osa vastaajista oli kirjoittanut kyselyssä huomioita kenttään, etteivät tienneet, mikä toipumissuunnitelma on. Tästä saattoi päätellä, ettei sellaista olekaan tai ainakaan sen olemassaolosta ei ole tiedotettu henkilökunnalle riittävästi. Toipumissuunnitelma on dokumentti, jossa on ohjeita ja suunnitelmia tietoturvaonnettomuuksista selviämiseksi.

Taulukko 9. Tietoturvakysely, salasanatietoutta

Salasana	qwerty123456	h5s6j	fgUw7Fkd8d	0rgan1saat10n n1m1
Ylin	8	10	10	8
Keskiarvo	4,2	6,1	4,9	4,8
Alin	1	3	1	1

Taulukossa 9 näkee tulokset kysymykselle, jossa salasanoille piti antaa arvosana asteikolla 1-10, jossa 10 tarkoittaa hyvää ja 1 huonoa. Käyttäjätunnuksen oletettiin olevan fgUw7Fkd8d. Kaikki salasanat ovat huonoja. qwerty123456 muodostuu näppäimistön mukaan ja on siksi huono. h5s6j on salasanaksi liian lyhyt ja fgUw7Fkd8d, joka on sinänsä todella hyvä salasana, oli sama kuin käyttäjätunnus ja tämän vuoksi huonoin kyseisistä salasanoista. On huolestuttavaa, että monet pitivät salasanoja hyvinä, mutta onneksi noin puolet vastanneista piti salasanoja huonoina. Salasanan fgUw7Fkd8d kohdalla osa ei välttämättä huomannut sen olevan sama kuin ilmoitettu käyttäjätunnus, joten sen saamat korkeat arvosanat eivät välttämättä kerro mitään. 0rgan1saat10n n1m1 oli alun perin Yhdistys X:n nimi, jossa osa kirjaimista oli vaihdettu numeroiksi. Vaihdoin salasanan tietoturvasyistä tällaiseksi, jottei Yhdistys X:n nimi käy siitä ilmi.

Kyselyssä kysyttiin vielä tiedostojen poistamisesta. Kysymykseen ”Poistuuko tiedosto, jos laitat sen roskakoriin”, vastattiin vain ei. Aikaisemmin yksi henkilö ei ollut asiasta varma. Kysymykseen ”Poistuuko tiedosto, jos tyhjennät roskakorin”, kymmenen henkilöä valitsi kyllä. Tiedosto ei kuitenkaan poistu roskakoria tyhjennettäessä. Tämän tiesi vain neljä henkilöä. Yhdysvaltain puolustusministeriön julkaiseman dokumentin U.S. DoD Unclassified Computer Hard Drive Disposition mukaan tieto täytyy päällekirjoittaa, kiintolevy pitää tuhota tai kiintolevyn magneettisuus pitää poistaa siihen soveltuvalla laitteella (Information Assurance Support Environment 2001). Päällekirjoittamisella tarkoitetaan uuden, merkityksettömän tiedon laittamista vanhan tiedon päälle. Jos tietoa ei tuhota kunnolla, sen voi palauttaa esimerkiksi Piriform nimisen yrityksen ilmaisella Recuva ohjelmalla.

Kun kyselin Yhdistys X:n henkilökunnalta, minkälaisia tietoturvaohjeita heille on annettu, kukaan ei osannut vastata mitään. Edes johto ei tiennyt asiasta juuri mitään. Tietoturvaohjeita ei siis ollut tai ne olivat kadonneet ja unohtuneet.

3.4.3 Laiteturvallisuus

Laiteturvallisuudella tarkoitetaan fyysisten laitteiden, kuten tietokoneiden, tulostimien ja johtojen turvallisuutta. Tavoitteena on estää laitteiden vahingoittumiset, häviämiset, varastamiset ja muut organisaation toiminnalle haitalliset laitteisiin liittyvät tapahtumat. Laiteturvallisuutta voidaan saavuttaa sijoittamalla laitteet siten, että ulkopuoliset eivät pääse niihin helposti käsiksi. Kuumenevat laitteen pitää sijoittaa siten, että niiden ilmastointi tai jäähdytys toimii ja ne eivät sytytä mitään palamaan. Laitteet pitää myös suojata sähkökatkoilta. Laitteiston säännöllinen huolto auttaa suojautumaan niihin liittyviltä riskeiltä. On myös otettava huomioon toimitilojen ulkopuolelle vietävät laitteet ja niihin liittyvät suuremmat katoamis- ja varastamisriskit. Kun laitteisto poistetaan käytöstä, on pidettävä huolta, että niihin ei jää luottamuksellisia tietoja. (ISO/IEC 27001 2005.)

Tutkin laitteisiin liittyvää turvallisuutta ja huomasin lukuisia puutteita. Sisäisen verkon palvelin sijaitsi aivan ulko-oven vieressä, lukitsemattomassa tilassa, joka oli usein myös auki. Tila oli ilmastoitu, mutta oven auki pitäminen haittasi ilmastointia hieman. Vaikka ulko-ovi oli lukossa, asiakkaat saivat välillä kulkea vapaasti käytävillä, varsinkin lähtiessään. Joku voisi rikkoa tai varastaa laitteistoa, joskin se olisi melko epätodennäköistä.

Työasemat sijaitsivat erillään toisista. Useimmat koneista kävivät normaalisti, mutta osa niistä vaikutti kuumilta. Minkäänlaista ylikuumenemista ei kuitenkaan esiintynyt. Mittasin lämpötilat käyttäen Piriform yrityksen ilmaista Speccy nimistä ohjelmaa, joka näyttää järjestelmän osien lämpötilat. Tarkistin lämmöt vain niistä koneista, joiden tuulettimet pitivät kovaa ääntä. Vertasin lämpöjä valmistajien sivuilla oleviin määrityksiin. Lämpötilat olivat riittävän alhaiset.

USB-muistitikkuihin tallennettiin välillä salaisia tietoja. Samoja USB-muistitikkuja käytettiin työmatkoilla. Muistitikku on niin pieni, että se saattaa helposti pudota tai unohtua jonnekin. Sen löytäjä saa tiedot haltuunsa, varsinkin jos tietoja ei ole salattu mitenkään. Vanhat, normaalilla tavalla poistetut tiedostotkin voitaisiin mahdollisesti vielä palauttaa.

Kannettavilta tietokoneiltakin löytyi salassa pidettävää tietoa. Huoltaessani koneita harjoittelun aikana, huomasin vanhoja tiedostoja, joissa oli asiakkaiden tietoja. Työmatkalla käytettävä kannettava tietokone saatetaan varastaa. Esimerkiksi Floridan yliopiston kannettava, joka sisälsi 8 300 opiskelijan ja työntekijän tietoja, kuten nimiä, henkilötunnuksia ja jopa ajokortin numeroita, varastettiin (UPI 2010).

3.4.4 Verkkoturvallisuus

Koska valitsin tietojärjestelmät suuntautumisvaihtoehdon enkä tietoliikenne suuntautumisvaihtoehtoa, rajasin projektia siten, että en puutu verkon rakenteeseen tai sen asetuksiin.

3.4.5 Varmuuskopiointi

Tärkeät tiedot täytyy varmuuskopioida. Sen tavoitteena on tietojen eheyden ja saatavuuden takaaminen, ja siten myös organisaation toiminnan jatkuvuuden turvaaminen. Varmuuskopioiden täytyy sijaita erillään alkuperäisistä tiedoista. Ne pitää myös suojata kuten alkuperäiset tiedot. On oltava dokumentti, josta selviää täsmälleen, kuinka varmuuskopioidut tiedot palautetaan. Varmuuskopioiden palauttamisen toimivuutta kannattaa testata säännöllisesti. Automatisointi helpottaa ja nopeuttaa varmuuskopiointia. (ISO/IEC 17799 2000.)

Suurin osa Yhdistys X:n tiedoista sijaitsi palvelimella, jonka tiedot varmuuskopioitiin säännöllisesti. Varmuuskopiot sijaitsivat kuitenkin samassa

huoneessa palvelimen kanssa. Tulipalon sattuessa, joka saattaisi johtua vaikka ylikuumentuneesta palvelimesta, sekä palvelin että varmuuskopiot tuhoutuisivat ja kaikki tiedot menetettäisiin. Tämä aiheuttaisi ymmärrettävästi huomattavia ongelmia.

Osa tiedoista sijaitsi kuitenkin työasemilla ja muistitikuilla. Näitä tietoja ei käytännössä varmuuskopioitu mitenkään. Tietojen tuhoutuessa, esimerkiksi kiintolevyn tai USB-muistitikun hajotessa, tiedot saatettaisiin menettää lopullisesti.

4 TIETOTURVATASON NOSTAMINEN

Tietoturvatason nostaminen tapahtuu siten, että suunnitellaan menetelmiä, joilla riskejä voidaan poistaa, pienentää tai harventaa. Hyvään tietoturvatasoon kuuluu myös varautuminen mahdollisiin riskeihin. Tuottamani tietoturvadokumentit tallennettiin Yhdistys X:n intranetiin, josta ne ovat saatavissa koko henkilökunnalle.

4.1 Ohjelmistojen päivitys

Ensimmäiseksi sovin kaikkien kanssa ajat, jolloin voin päivittää tietokoneiden käyttöjärjestelmät, tietoturvasovellukset ja mahdolliset muut ohjelmat. Ohjelmistojen päivittäminen kesti välillä hyvin kauan, koska puuttuvia päivityksiä oli hyvin paljon ja tietokoneet olivat hitaita. Samalla suoritin muitakin perushuoltotoimenpiteitä. Joissain koneissa Windows XP:n päivityksiä ei voinut asentaa Windows updaten kautta, joka on Microsoftin automaattinen päivitysten lataus- ja asennuspalvelu. Windows update ilmoitti virheitä, joiden avulla löysin ratkaisun Microsoftin tukipalvelusta. Asensin manuaalisesti päivityksiä, joiden jälkeen pystyin päivittämään Windows Updaten. Tämän jälkeen Windows update toimi normaalisti. Tietoturvasovelluksien päivittäminen sujui ongelmitta.

Windows XP:n olisi ollut hyvä vaihtaa uudempaan Windows 7 käyttöjärjestelmään. Tulimme kuitenkin siihen tulokseen, että Yhdistys X:n tiukan taloudellisen tilanteen vuoksi käyttöjärjestelmää ei kannata vielä vaihtaa. Vaihto kannattaa tehdä vasta sen jälkeen, kun Microsoft lopettaa Windows XP:n tuen ja päivitykset 8.4.2014 (Microsoft 2010).

Ohjelmistot eivät kuitenkaan pysy ajantasaisina itsestään. Automaattiset päivitystoiminnot auttavat hieman, mutta eivät selvästikään olleet toimineet täydellisesti. Tämän vuoksi tein ehdotuksen, että joku henkilökunnan jäsen pitää huolta päivityksistä ja tarkistaa tietokoneet tietyn väliajoin. Valmistin myös ohjeet päivitysten tarkastamista ja asennusta varten.

Virustorjunnan, palomuurin ja Microsoftin tuotteiden lisäksi tietokoneilla oli useita muita sovelluksia, kuten IZArc -pakkausohjelma, dvd-levyjen kirjoitusohjelma, winzip –paukkausohjelma. Näiden sovellusten päivitysten jatkuva tarkistaminen olisi työlästä. Niiden merkitys on myös huomattavasti vähäisempi, koska ne ovat yksinkertaisia ja niitä käytetään vain luotettavien tiedostojen kanssa.

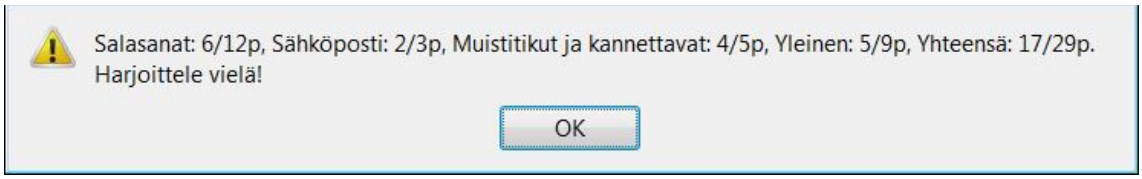
4.2 Tietoturvakoulutus

Pidin 27 dian esityksen tietoturvasta ja sen tilasta Yhdistys X:ssä. Esityksessä käsittelin ensin lyhyesti, mitä tietoturva on. Tämän jälkeen kävin läpi tekemäni tietoturvakyselyn tuloksia ja kerroin oikeat vastaukset. Selitin, miksi sen hetkinen tietoturvatilanne oli huono ja kävin läpi tietoturvan puutteita. Kerroin myös lyhyesti alustavista parannusehdotuksista ja näytin hahmotelman eri materiaaleista, joita aioin tuottaa. Lopuksi esitin vielä esimerkkejä tietoturvaonnettomuuksista, joita oli tapahtunut ympäri maailmaa.

Valmistin lisäksi HTML-muotoisen nimettömän testin, joka ei tallenna tuloksia. Testissä oli 29 kyllä/ei ja hyvä/huono kysymystä. Kysymykset liittyivät sähköpostin käyttöön, salasanoihin, kannettaviin tietokoneisiin, USB-muistitikkuihin ja yleiseen tietoturvaan. Taulukossa 10 on listattu joitakin tietoturvatestin kysymyksiä. Vastauksen jälkeen testi kertoo vastaajalle, oliko vastaus oikein vai väärin ja kertoo sille syyn. Lopuksi testi näyttää yhteenvedot tuloksista, esimerkiksi kuva 4. Testin tarkoituksena on toimia opetus- ja mittausvälineenä, jota jokainen voi käyttää itsenäisesti.

Taulukko 10. Esimerkkejä tietoturvatestin kysymyksistä

Kysymys	Oikea vastaus
Henkilö soittaa ja kertoo olevansa vastuussa organisaation tietojärjestelmien ylläpidosta. Hän tarvitsee salasanan ja käyttäjätunnukset nopeasti korjatakseen vian. Ne kannattaa antaa hänelle heti.	Ei
Hyvä ja päivitetty tietoturva- ja virustorjuntaohjelma suojaa kaikilta viruksilta	Ei
Kaikki tulosteet voi heittää roskikseen	Ei
Kun käytän tiedostojen tuhoamisohjelmaa, tiedosto poistuu varmasti muistitikulta	Ei
Tiedot.doc.exe on turvallinen liitetiedosto tutulta lähettäjältä	Ei
Sama salasana useassa eri kohteessa muistamisen helpottamiseksi	Ei
Salatut muistitikut ovat turvallinen tapa siirtää henkilötietoja kahden koneen välillä	Kyllä



Kuva 4. Esimerkki tietoturvatestin tuloksista

Testin ei ole tarkoitus olla kaiken kattava tietoturvaymmärryksen mittari. Se auttaa testin suorittajaa muistamaan tietoturvaan liittyviä asioita. Liitteessä 1 on lisää kysymyksiä, joista osa on muutettu organisaation nimen piilottamiseksi tietoturvasyistä.

4.3 Ohjeistus ja säännöt

Jos organisaatiossa ei ole lainkaan kirjallisia tietoturvasääntöjä tai ohjeita, on hyvin ymmärrettävää, että henkilökunta ei toimi tietoturvallisesti, vaikka heitä kuinka kouluttaisi tietoturva-asioista. Koulutus unohtuu helposti, mutta ohjeet auttavat muistamaan. Ne eivät saa olla liian pitkiä tai monimutkaisia, koska se hidastaa niiden käyttöä ja vaikeuttaa niiden ymmärtämistä. Ohjeet eivät saa myöskään olla liian rajoittavia tai niitä ei haluta tai jakseta noudattaa. (Microsoft TechNet 2010.)

Ohjeiden täytyy olla jokaisen henkilökuntaan kuuluvan helposti saatavilla. Henkilökunnan täytyy myös tietää, että sellaiset ovat olemassa ja että niitä täytyy noudattaa. Tämä vaatii johdolta halua sitoutua tietoturvaan. (Calder & Watkins 2005, 13.)

Monet eivät usko, että kukaan voisi hyötyä oman organisaationsa tiedoista ja tunnuksista. Tämä helpottaa huomattavasti rikollisten toimintaa, jotka saattavat kaapata organisaation tietokoneet valtaansa kenenkään tietämättä ja käyttää niitä esimerkiksi roskapostin lähettämiseen. Asiaan uskotaan vasta kun se tapahtuu, jolloin on jo liian myöhäistä ja vahingot on kärsitty. Ohjeiden tarkoituksena onkin antaa organisaation johdolle ymmärrys siitä, että tietoturva on tärkeää ja sen olemassa olo organisaatiossa on heidän vastuullaan. (Microsoft TechNet.)

Koska ohjeita ei ollut, päätin tehdä A4-kokoisen muistilistan, joka sisälsi yleisiä tietoturvaohjeita. Käytin muistilistan laatimisessa apuna Tietoyhteiskunnan kehittämiskeskus ry:n tietoturvaopasta (TIEKE 2010). Ohjeissa käsiteltiin mm. Internetiä, sähköpostin käyttöä, USB-muistitikkuja, kannettavia tietokoneita, tulostamista ja ongelmatilanteessa toimimista.

Tämän jälkeen laadin vielä erillisen A4-kokoisen salasanamuistilistan, josta kävi ilmi, mikä on hyvä salasana, miten sitä käytetään ja säilytetään sekä kuinka se muistetaan.

Auttaakseni johtoa sitoutumaan tietoturvan parantamiseen ja ylläpitoon, valmistin lyhyen dokumentin, joka sisälsi ohjeita hallinnolle. Ohjeet perustuivat omiin päätelmiini sekä Microsoftin TechNet artikkeliin 10 Immutable Laws of Security Administration (Microsoft TechNet). Ohjeessa kerrotaan että on johdon vastuulla, että henkilökunta noudattaa tietoturvaohjeita.

Paraskaan tietoturva ei ylläpidä itseään. Vaikka nykyinen johto osaisikin ylläpitää sitä, johdon vaihtuessa tietoturvan ylläpito voi lakata. Myös muu henkilökunta voi vaihtua. Tämän vuoksi on tärkeää, että johdolla on saatavilla dokumentti, josta käy ilmi tarvittavat tietoturvaan liittyvät tehtävät, joiden toteutumisesta heidän täytyy vastata. Valmistin lyhyen dokumentin asiaan

liittyen. Dokumentissa kerrotaan ohjelmistojen päivittämisestä, henkilökunnan tietoturvaymmärryksen ylläpidosta sekä edellytykset tietoturvan ylläpitämiseksi.

4.4 Luottamuksellisien tietojen suojaus ja hävittäminen

Luottamuksellisia tietoja sisältävät tiedostot ovat aina riski organisaatiolle ja kun ne poistetaan, ne kannattaa poistaa päällekirjoittamalla, jolloin niistä ei jää mitään jäljelle. On hyvä tietää, että muistitikkujen päällekirjoittaminen ei onnistu ilman, että koko muistitikku kirjoitetaan täyteen tietoa. Tämä johtuu muistitikkujen rakenteesta ja on hyvin hidasta ja vähentää muistitikun käyttöikää. On myös huomioitava, että tiedostojen suuri koko ja määrä hidastavat päällekirjoittamista. Tavallisia tiedostoja, jotka eivät sisällö luottamuksellisia tietoja, ei kannata turhaan poistaa päällekirjoittamalla. Tämä veisi vain turhaan aikaa. Koska tiedostojen tuhoaminen muistitikuilta on vaikeaa, kannattaa luottamukselliset tiedostot salata. Kokonaan salattujen muistitikkujen luominen on työlästä. (Eraser 2010.)

En kuitenkaan olettanut, että jokainen osaa suorittaa tiedostojen päällekirjoituksen, joten valmistin lyhyen ohjeen, jonka avulla voi ladata, asentaa ja konfiguroida ilmaisen, avoimeen lähdekoodiin perustuvan tiedostojen päällekirjoitusohjelman, Eraserin. Itse ohjelman käyttö on helppoa ja vaivatonta, mutta sekin on käsitelty ohjeissa. Lisäsin ohjeen perään huomioita päällekirjoittamisesta.

Työasemien, palvelimien, kannettavien tietokoneiden ja muistitikkujen tiedot voi suojata salaamalla ne. Ilmainen avoimeen lähdekoodin perustuva TrueCrypt sopii hyvin tähän tarkoitukseen. Se salaa tiedot sotkemalla ne lukukelvottomaksi annetun salasanan perusteella ja niiden palauttaminen ymmärrettäväksi vaatii saman salasanan syöttämien ohjelmaan. Ohjelmalla voi salata koko laitteen, jolloin kaikki tiedot salataan automaattisesti ilman, että niiden käyttö tai käsittely hankaloituisi. Toinen mahdollisuus on luoda salattu tiedosto, johon halutut tiedostot voidaan tallentaa salattuna. Tämä on kuitenkin

hieman työläämpää ja mahdollistaa virheet, jos käyttäjä tallentaa vahingossa luottamukselliset tiedot salaamattomana tavalliseen paikkaan. Ohjelmalla salattua tietoa ei voi saada mitenkään selville ilman salasanaa, joten sitä ei kannata hävittää. Tämä tarkoittaisi käytännössä tiedon menetystä. Vaikka tieto olisikin vielä olemassa, sitä ei kuitenkaan voisi käyttää mitenkään. (TrueCrypt 2010.)

Kannattaa huomioida, että salatun muistitikun tietojen lukeminen vaatii salasanan lisäksi TrueCrypt ohjelman tietokoneelle asennettuna. On myös olemassa valmiiksi salattuja, turvalliseen käyttöön tarkoitettuja muistitikkuja, joihin on valmiiksi asennettuna muistitikulta toimiva salausohjelma. Tällöin tietokoneelle, jolla muistitikkua käyttää, ei tarvitse asentaa mitään. (TrueCrypt 2010.)

Muistitikkujen salauksen vaikeuden vuoksi kannattaa luoda salattuja arkistotiedostoja, kuten .zip tai .rar, jotka voivat sisältää muita tiedostoja. IZArc on pakkaus- ja arkistointiohjelma, joka on ilmainen myös organisaatioille. Sillä voi pakata ja salata tiedostoja ja kansioita, ja siinä on hyvin laajat ominaisuudet. Pakatut ja salatut tiedostot pitää ensin purkaa IZArc:lla tai vastaavalla ohjelmalla, ennen kuin niitä voi käyttää. Purkamisella tarkoitetaan tässä tapauksessa salauksen ja pakkaamisen poistoa. Tehdäkseen tämän, täytyy ensin tietää salasana, joka asetettiin tiedostoja salatessa. (Zahariev I 2010.)

Valmistamissani tiedostojen salaamis- ja IZArc ohjeissa kerrotaan lisäksi, että tiedostot pitää salata ennen, kuin ne laitetaan tikulle. Kun ne puretaan, ne pitää purkaa tietokoneen kiintolevylle eikä muistitikulle. Muistitikulle purkaminen tarkoittaa käytännössä samaa kuin tiedoston tallentaminen sille.

Tiedostoja saatetaan joskus poistaa vahingossa. Piriform yrityksen ilmaisella Recuva ohjelmalla voi palauttaa poistettuja tiedostoja, kunhan niitä ei ole päällekirjoitettu. Mitä kauemmin tiedostojen poistosta on kulunut, sitä epätodennäköisempää on, että tiedostot voi palauttaa kokonaisina. Laadin ohjeet Recuva ohjelman käyttämiseksi.

4.5 Toipumissuunnitelma

Valmistin lyhyen, muutaman sivun mittaisen toipumissuunnitelman, johon listasin Yhdistys X:lle tärkeitä toimintoja ja tietoja. Kokosin listan kyselemällä henkilökunnalta, mitä he tekevät ja mitä tietoja he tarvitsevat työssään. Siinä on lueteltuna useita mahdollisia tietoturvaonnettomuuksia. Jokaisen kohdalle kirjoitin mahdollisia toimia, joita kannattaa noudattaa niiden toteutuessa. Organisaation hallinnon täytyy päivittää ja tarkentaa toipumissuunnitelmaa.

5 TULOSTEN TARKASTELU

Projektien tuloksia täytyy aina tarkastella, niin projektien aikana kuin niiden jälkeenkin. Näin saadaan selville, oliko projektista hyötyä, olivatko siinä käytetyt menetelmät oikeita ja miten jatkossa kannattaa menetellä. Tässä luvussa käsittelen projektin tuloksia noin puolen vuoden kuluttua sen toteutuksesta ja pohdin mahdollisia jatkotoimenpiteitä.

5.1 Tulokset

Organisaatiossa käydessäni huomasin heti, että osa työntekijöistä oli ottanut opikseen tietoturva-asioista. Eräs henkilö ei enää säilyttänyt salasanoja näyttöön teipattuna. Hän ei myöskään tallentanut niitä selaimen muistiin. Monet muistivat muistitikkujen ja sähköpostin vaarat. Valitettavasti oli myös poikkeuksiakin. Osa ei ollut sisäistänyt vielä paljonkaan asioita ja salasanoja säilytettiin huonosti.

Organisaation hallinnon ja kirjanpidon puolella asiaa oli mietitty, mutta paljonkaan ei oltu vielä toteutettu. Minulta kysyttiin lisää neuvoja ja mielipiteitä, miten kannattaa menetellä. Tarkoituksena on tehdä tietoturvallisuusopas. Dokumentinhallintajärjestelmää harkitaan. Tämä helpottaisi tietojen luokittelua ja käyttöoikeuksien hallintaa huomattavasti. Myös käytön seuranta mahdollistuu.

Käyttöjärjestelmien päivitystä tulevaisuudessa harkitaan. Tämän toteutuessa vanhan käyttöjärjestelmän puutteista ja riskeistä päästään eroon ja päivitykset jatkuvat.

Myös salauksen käyttöä mietittiin ja se on tarkoitus ottaa käyttöön muistitikkuja ja sähköpostia käytettäessä. Varmuuskopiot ovat nyt paremmassa turvassa. Tietojen tallennuksen selkeyttä on ajateltu.

Tulokset olivat aika lailla sitä mitä odotinkin. Tietoturvatietoisuus nousi ja toiminta muuttui tietoturvallisemmaksi, mutta parannettavaa jäi huomattavasti.

Ohjeistus ja säännöt ovat käytössä, mutta niiden noudattaminen ei ole vielä kohdallaan. Tärkeintä oli, että tietoturvallisuutta alettiin ajatella.

5.2 Jatkotoimenpiteet

Koska Yhdistys X:n tietoturvatilanteeseen jäi parannettavaa, aion tarpeen vaatiessa toimia organisaation tukena tietoturvan kehittämisessä. Keskustelin organisaation kanssa tietoturvapolitiikasta ja sen merkityksestä. Tietoturvapolitiikkaa pidettiin turhana ja liian muodollisena. Pohdimme, että tietoturvapolitiikan kannattaa olla semmoinen, että se sopii organisaatiolle. Sen ei tarvitse olla hieno ja virallinen, vaan toimiva ja helposti ymmärrettävä. Tietoturvapolitiikka valmistetaan laatimiani ohjeita ja sääntöjä hyväksi käyttäen.

Organisaation johdon on vastattava suuresta osasta jatkotoimenpiteistä, kuten ohjeiden ja sääntöjen päivittämisestä ja tietoturvatason ylläpitämisestä ja nostamisesta. Uusille työntekijöille on annettava tietoturvadokumentit ja heidän täytyy sitoutua noudattamaan niitä.

6 LOPPUSANAT

Tietoturva aiheena on hyvin laaja. Projektia piti rajata vähän sieltä ja täältä, etenkin laitteiston ja verkon alueilta. Joskus tuntui, että työstä tulisi liian yleispätevä, jolloin mitään yksittäistä asiaa ei käsiteltäisi riittävän syvällisesti. Toisaalta, liiallinen standardeihin sotkeutuminen olisi haitannut toimeksiantajaa, joka ei tarvinnut hienoja ja virallisia dokumentteja, vaan oikeita, toimivia ja halvasti toteutettavissa olevia parannuksia ja ohjeita, joita he pystyvät itsekin kehittämään ja käyttämään.

Projektin tarkoituksena oli nostaa yhdistys X:n tietoturvan tasoa. Niin se myös teki, joten projekti oli onnistunut. Parannettavaa tietoturvassa jäi, mutta se oli odotettavissakin. En ikinä uskonutkaan, että yhdistyksen tietoturvasta tulisi täydellisyyttä hipova linnoitus. Projekti oli organisaatiolle hyödyksi ja se oli kaikken tärkeintä. Organisaatio sai pohjan ymmärrykselle ja kykenee nyt parantamaan asioita itsekin.

Opin itse myös paljon uutta tietoturvasta, tietoturvan kartoittamisesta ja sen tason nostamisesta. Huomasin myös, ettei se ole niin helppoa kuin voisi helposti luulla. Tietoturvaan liittyy monenlaisia pieniä, mutta tärkeitä asioita. Pienetkin asiat on huomioitava.

Osa asioista oli muodostunut minulle itsestäänselväksi yleistiedoksi, kuten ihmisen epäuskoisuus tietoturvauhkien toteutumiselle. Vuosien aikana olen nähnyt lukuisia uutisia, haastatteluja ja tutkimustuloksia tietoturvaan liittyvistä asioista. Olen myös huomannut asioita henkilökohtaisesti. Tämän vuoksi oli välillä vaikeaa kirjoittaa asioista, jotka olivat minulle itsestäänselviä, mutta eivät muille. Niille täytyi kuitenkin etsiä lähde.

LÄHTEET

AV-Comparatives.org 2010. Viitattu 17.10.2010
http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf

Baskerville, R.; Goodman, S.; Straub, D. 2008. Information Security. Policy, Processes and Practices. M.E. Sharpe Inc.

Hayes, B. 2003. Conducting a Security Audit: An Introductory Overview. Symantec. Viitattu 17.3.2011.2010 http://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview

Caelli, W; McCullagh, A. 2000. Non-Repudiation in the Digital Environment. Viitattu 16.3.2011 http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/778/687

Calder, A. 2005. Business Guide to Information Security. Lontoo: Kogan Page Limited.

Calder, A.; Watkins, S. 2005. IT Governance. A Manager's Guide to Data Security and BS 7799/ISO 17799. Lontoo: Kogan Page Limited.

Eraser. Viitattu 16.11.2010 http://eraser.heidi.ie/

Gregory, P. 2008. IT Disaster Recovery Planning For Dummies. John Wiley & Sons.

Information Assurance Support Environment 2001. Defense Information Systems Agency. Unclassified Computer Hard Drive Disposition. Viitattu 9.7.2010 http://iase.disa.mil/policy-guidance/asd_hd_disposition_memo060401.pdf

ISO (International Organization for Standardization). ISO/IEC 17799 2000.

ISO (International Organization for Standardization). ISO/IEC 27001 2005.

Maiwald, E.; Sieglein, W. 2002. Security Planning and Disaster Recovery. McGraw-Hill Professional.

Microsoft. 2010. Viitattu 12.10.2010 http://support.microsoft.com/lifecycle/?C2=1173

Microsoft TechNet. 2010. Viitattu 12.11.2010 http://technet.microsoft.com/en-us/library/cc722488.aspx

Raggad, B. G. 2009. Information Security Management. Concepts and Practice. Taylor and Francis.

Tietoturvaopas. 2010. Viitattu 18.11.2010
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/

TIEKE (Tietoyhteiskunnan kehittämiskeskus ry). 2010.
Viitattu 13.11.2010 http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/

TrueCrypt 2010. http://www.truecrypt.org

UPI (United Press International). 2010. Viitattu 12.11.2010
http://www.upi.com/Science_News/2010/09/01/Stolen-university-laptop-had-personal-info/UPI-53951283365552/

VTT. 2009. Viitattu 12.11.2010 http://virtual.vtt.fi/virtual/riskianalyysit/index273b.html

Zahariev I. Viitattu 13.11.2010 http://www.izarc.org/index.html

Tietoturvatesti

Tietoja ei tallenneta. Vastaa kuhunkin kysymykseen vain kerran. Pyri saamaan täydet pisteet.

Salasana

Ovatko seuraavat salasanat hyviä, kun käyttäjätunnus on alu7H34fr9

0rgan1saat10	arkku	gsdkl48GH3	Peräkärry	salasana	alu7H34fr9	Akfku5/(hT3

Mitkä seuraavista ovat hyviä/huonoja salasanakäytäntöjä?

Salasana teipattuna koneen näyttöön	Salasana lompakossa ilman käyttäjätunnusta	Ei käytetä salasanoja ollenkaan	Salasanan vaihto muutaman kuukauden välein	Sama salasana useassa eri kohteessa muistamisen helpottamiseksi

---

Sähköposti

Ovatko seuraavat väittämät totta?

työ.doc.exe on turvallinen liitetiedosto tutulta lähettäjältä	Jos viestin lähettäjänä on joku@organisaatio.fi, viesti on varmasti organisaation henkilökunnalta	Sähköpostilla on turvallista lähettää henkilötietoja

---

Muistitikut ja kannettavat

Ovatko seuraavat väittämät totta?

Muistitikut ovat turvallinen tapa siirtää henkilötietoja kahden koneen välillä	Salatut muistitikut ovat turvallinen tapa siirtää henkilötietoja kahden koneen välillä	Kun poistan henkilötiedot kannettavassa ja tyhjennän roskakorin, tiedot ovat poissa	Luottamuksellisten tietojen käsittely bussissa, junassa tai lentokoneessa kannettavan kanssa on huoleton tapa säästää aikaa	Kun käytän tiedostojen tuhoamisohjelmaa, tiedosto poistuu varmasti muistitikulta

---

Yleinen

Ovatko seuraavat väittämät totta?

Tietokone kannattaa lukita, kun käy vessassa	Varmuuskopioita on hyvä säilyttää palvelinhuoneessa, jotta tiedot voi nopeasti palauttaa ongelman sattuessa	Kaikki tulosteet voi heittää roskikseen	Hyvä ja päivitetty tietoturva- ja virustorjuntaohjelma suojaa kaikilta viruksilta	Tärkeitä papereita ei pidä säilyttää pöydällä
Kun asiakkaalle näyttää tietoja näytöltä, on varottava, ettei hän näe vahingossa muiden ihmisten tietoja	Kun keskustelee asiakkaan kanssa puhelimessa luottamuksellisista asioista, ovea ei tarvitse sulkea	Henkilö soittaa ja kertoo olevansa vastuussa organisaation tietojärjestelmien ylläpidosta. Hän tarvitsee salasanan ja käyttäjätunnukset nopeasti korjatakseen vian. Ne kannattaa antaa hänelle heti.	Kaikki suomenkieliset sivustot ovat turvallisia	

Windowsin ja muiden ohjelmien päivitykset

Päivitysten asentaminen

Windows, Office ohjelmat ja Internet Explorer

Manuaalinen päivitys

1. Valitse **Käynnistä** valikosta **Windows Update –sivusto** tai **Microsoft Update**
2. Toimi ohjeiden mukaan ja valitse **Pika-asennus**

Automaattiset päivitykset

1. Oikealle alhaalle tulee ilmoitus, että päivitykset ovat asennettavissa, klikkaa sitä
   Päivitykset saattavat asentua myös itsestään

Antivirus

1. Klikkaa hiiren kakkosnäppäimellä oikealla alhaalla olevaa  (symantec endpoint protection) ja valitse **Open Symantec Endpoint Protection**
2. Valitse **Live Update** – ohjelma päivittää itsensä

Google Chrome internet selain

1. Jos koneeseen on asennettu Google Chrome selain, avaa se
2. Klikkaa oikealta ylhäältä jakoavaimen kuvaa ja valitse Tietoja Google Chromesta
3. Chrome ilmoittaa, jos uusia päivityksiä on tullut. Toimi ohjeiden mukaan

SALASANA

Hyvä salasana

- **Vähintään 8 merkkiä pitkä, mieluummin 12**
- **Ei sisällä minkään kielen sanaa, nimiä, päivämääriä tai mitään arvattavissa olevaa**
- **Ei muodostu näppäimistön mukaan, esim. asdf1234**
- **Ei ole oppaassa esiintyvä esimerkkisalasana**
- **Sisältää vähintään kolmea seuraavista: Isot kirjaimet, pienet kirjaimet, numerot, erikoismerkit**
- **Ei ole sama kuin käyttäjätunnus eikä sisällä sitä**

Salasanan käyttö ja säilytys

- **Tärkeissä kohteissa kuten pankki, sähköposti, tietokoneet ja organisaation www-sivut, on käytettävä eri salasanoja**
- **Salasanaa ei pidä tallentaa tietokoneen selaimen muistiin**
- **Pidä huolta, ettei kukaan näe, kun näppäilet salasanasi**
- **Älä anna salasanaasi kenellekään, äläkä varsinkaan sähköpostin kautta**
- **Älä säilytä salasanaasi helposti löydettävällä muistilapulla**
    - Jos pakko, säilytä esimerkiksi lompakossa, muttei käyttäjätunnuksen kanssa
- **Vaihda salasanasi heti, jos on uskot, että se on paljastunut, harkitse muidenkin vaihtamista**
- **Jos koneellasi on tiedosto, johon keräät käyttäjätunnuksia ja salasanoja, suojaa se salasanalla, jonka MUISTAT VARMASTI**

Salasanan muistaminen

- **Jos salasanojen muistaminen on vaikeaa, voit kehittää muistisäännön (saattaa heikentää salasanaa)**
    - Esim. palvelun/kohteen kolme ensimmäistä kirjainta, jonkin helposti muistettavan lauseen jokaisen kirjaimen ensimmäinen sana ja kolmen merkin ulkoa opeteltava merkkijono
    - Sähköposti → Säh, *”Ain laulain työtäs tee”* → Altt, merkkijono 11s = **SähAltt11s**
    - Tietokone → Tie, ”*Ain laulain työtäs tee”* → *Altt, merkkijono 8x8* = TieAltt8x8
- **Älä paljasta muistisääntöä kenellekään**
- **Muistisääntö ei saa olla arvattavissa**
- **Älä käytä tätä esimerkkimuistisääntöä**